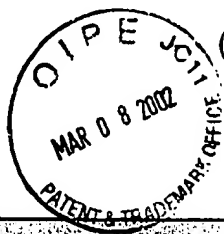


INFORMATION DISCLOSURE CITATION IN AN APPLICATION



(PTO-1449)

ATTY. DOCKET NO.
50325-0550

SERIAL NO.
09/955,902

COPY OF PAPERS
ORIGINALLY FILED

APPLICANT
Mihailo M. Stojancic, et al.

FILING DATE
September 18, 2001

GROUP
2131

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	PATENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE
LBC	5,928,315	7/27/99	Kobayashi et al.	708	491	9/12/97
LBC	5,982,900	11/9/99	Ebihara et al.	380	30	4/4/97
LBC	6,064,740	5/16/00	Curiger et al.	380	265	11/12/97

RECEIVED

MAR 13 2002

Technology Center 2100

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	PATENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

LBC	B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", (New York: John Wiley & Sons), 2 nd ed. 1996, pp. 246-250, pp. 466-474, pp. 483-494.

EXAMINER

Long Chen

DATE CONSIDERED

12/01/2004

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

Form PTO-1449 (modified) List of Patents and Publications For Applicant's Information Disclosure Statement (Use several sheets if necessary)			ATTY. DOCKET NO: 5150-43200		SERIAL NO: 09/560,695		
APPLICANT: Rajagopal et al.							
FILING DATE: April 27, 2000					GROUP: 2759		
U.S. PATENT DOCUMENTS							
EXAM. INITIALS	REF. DES	DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE

OIPE JCA1
 DEC 27 2001
 PATENT & TRADEMARK OFFICE

RECEIVED
 DEC 28 2001
 Technology Center 2100

FOREIGN PATENT DOCUMENTS							
EXAM. INITIALS	REF. DES	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUB CLASS	TRANSLATION. YES/NO

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)		
LBC	A1	Andrea Califano and Rakesh Mohan, "Multidimensional Indexing for Recognizing Visual Shapes", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 16, No. 4, April 1994, pgs. 373-392.
LBC	A2	Sameer A. Nene and Shree K. Nayar, "A Simple Algorithm of Nearest Neighbor Search in High Dimensions", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, No. 9, September 1997, pgs. 989-1003.
LBC	A3	Jon Louis Bentley, "Multidimensional Binary Search Trees Used for Associative Searching", Communications of the ACM, September 1975, Vol. 18, No. 9, pgs. 509-517.
LBC	A4	Jon Louis Bentley et al., "Optimal Expected-Time Algorithms for Closest Point Problems", ACM Transactions on Mathematical Software, Vol. 6, No. 4, December 1980, pgs. 563-580.

EXAMINER: <i>Longbin Chen</i>	DATE CONSIDERED: <i>12/02/2004</i>
-------------------------------	------------------------------------

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to the patent owner.

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)



ATTY. DOCKET NO.
50325-0550

SERIAL NO.
09/955,902

APPLICANT
Mihailo M. Stojancic, et al.

FILING DATE
September 18, 2001

GROUP
2131

U.S. PATENT DOCUMENTS

EXAMINER'S INITIALS	PATENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE

FOREIGN PATENT DOCUMENTS

EXAMINER'S INITIALS	PATENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						Yes	No

OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)

<i>LBC</i>	Cornell University, Computer Science Department, entitled "A Parallel Implementation of RSA", by David Pearson, dated July 22, 1996, (pgs. 1-10)
	IEEE Transactions on Computers, Vol. 47, No. 7, entitled "An RNS Montgomery Modular Multiplication Algorithm", by Jean-Claude Bajard, et al., © 1998 IEEE, dated July 1998, (pgs. 766-776)
	IEEE Transactions on Parallel and Distributed Systems, Vol. 6, No. 5, entitled "Modulo Reduction in Residue Number Systems", by Karl C. Posch, et al., © 1995 IEEE, dated May 1995, (pgs. 449-454)
	Swiss Federal Institute of Technology (ETH), Integrated Systems Laboratory, entitled "Efficient VLSI Implementation of Modulo $(2n \pm 1)$ Addition and Multiplication", by Reto Zimmerman, undated, (10 pgs.)
	RSA Laboratories, RSA Data Security, Inc., entitled "RSA Hardware Implementation", by Cetin Kaya Koc, Copyright © RSA Laboratories, Version 1.0, dated August 1995, (pgs. 1-28)
	Electrical & Computer Engineering, Oregon State University, entitled "A Scalable Architecture for Montgomery Multiplication", by Alexandre F. Tenca and Cetin K. Koc, undated, (15 pgs.)
	Proceedings of the 29 th Asilomar Conference on Signals, Systems and Computers, School of Electrical Engineering, University of Oklahoma, entitled "A Table-Lookup Scheme for Residue-to-Binary Conversion", by Chad C. Lamb and L.S. DeBrunner, © 1996 IEEE, (pgs. 214-217)
	TIMA Laboratory, entitled "Hardware for Computing Modular Multiplication Algorithm", by Alvaro Bernal and Alain Guyot, undated, (4 pgs)
	Dept. Electrical & Electronic Eng., University of Adelaide and Electronic Engineering Division, Cardiff University, entitled "Implementing 1,024-bit RSA Exponentiation on a 32-bit Processor Core", by B.J. Phillips and N. Burgess, © 2000 IEEE, (11 pgs)
<i>LBC</i>	LIM-URA CNRS 1787, CMI, Universite de Provence, France and Dept. of Math and Computer Science, University of Odense, Denmark, entitled "An RNS Montgomery Modular Multiplication Algorithm", by Jean-Claude Bajard, et al., © 1997 IEEE, (pgs. 234-239)

EXAMINER

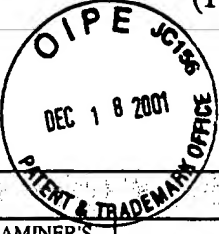
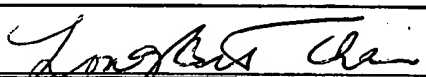
Longbin Chen

DATE CONSIDERED

12/02/2004

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.

RECEIVED
DEC 21 2001
Technology Center 2100

INFORMATION DISCLOSURE CITATION IN AN APPLICATION (PTO-1449)				ATTY. DOCKET NO. 50325-0550		SERIAL NO. 09/955,902	
				APPLICANT Mihailo M. Stojancic, et al.			
				FILING DATE September 18, 2001		GROUP 2131	
				U.S. PATENT DOCUMENTS			
EXAMINER'S INITIALS	PATENT NO.	DATE	NAME	CLASS	SUBCLASS	FILING DATE	
FOREIGN PATENT DOCUMENTS							
EXAMINER'S INITIALS	PATENT NO.	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						Yes	No
OTHER ART (Including Author, Title, Date, Pertinent Pages, Etc.)							
<i>LBC</i>	LIRMM, Montpellier, France, Universite de Bretagne Occidentale, Brest, France, and SDU/Odense University, Denmark, entitled "Montgomery Modular Multiplication in Residue Arithmetic", by Jean-Claude Bajard, et al., dated November 1, 2000, (pgs. 1-11)						
	LIRMM, Montpellier, France, Universite de Bretagne Occidentale, Brest, France, and SDU/Odense University, Denmark, entitled "Modular Multiplication and Base Extensions in Residue Number Systems", by Jean-Claude Bajard, et al., undated, (7 pgs)						
	Digital Equipment Corp., Paris Research Laboratory (PRL), entitled "Fast Implementations of RSA Cryptography", by M. Shand, et al., undated, (9 pgs)						
<i>LBC</i>	Thesis of Tolga Acar, Electrical & Computer Engineering, Oregon State University, entitled "High-Speed Algorithms & Architectures For Number-Theoretic Cryptosystems", by Tolga Acar, dated December 4, 1997 © by Tolga Acar 1997, (92 pgs)						
EXAMINER				DATE CONSIDERED 6/2/2004			

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.